

WHAT IS CLAIMED IS:

1. An apparatus for encrypting block data comprising:

encrypting sections connected in series, each of
5 the encrypting sections comprising:

a first unit configured to randomize first
subblock data which are obtained by dividing the block
data; and

a second unit configured to diffuse data output
10 from the first unit with respect to a range which is
wider than a range of the first subblock data and
supply a result of diffusion to a first unit in a
succeeding encrypting section, at least one bit of data
input to the first unit in own encrypting section being
15 transmitted to at least one bit of data input to the
first unit in the succeeding encrypting section via at
least two routes.

2. The apparatus according to claim 1, wherein
the at least one bit is present in each of the block
20 data.

3. The apparatus according to claim 1, wherein,
for each of all combinations of one bit selected from
the data input to the first unit in the own encrypting
section and one bit selected from the block data input
25 to the first unit in the succeeding encrypting section
or for some of the combinations which meet a
predetermined condition, one bit of the data input to

the first unit in the own encrypting section is transmitted to one bit of the data input to the first unit in the succeeding encrypting section via at least two routes.

- 5 4. An apparatus for encrypting block data comprising:

encrypting sections connected in series, each of the encrypting sections comprising:

- 10 first nonlinear transformation units configured to perform a nonlinear transformation process over first subblock data which are obtained by dividing the block data; and

- 15 a first linear diffusion unit configured to perform a linear diffusion process over data output from the first nonlinear transformation units with respect to a range which is wider than a range of the first subblock data and supply a result of diffusion to first nonlinear transformation units in a succeeding encrypting section,

- 20 wherein each of the first nonlinear transformation units comprises:

- 25 second nonlinear transformation units configured to perform a nonlinear transformation process over second subblock data which are obtained by dividing the first subblock data; and

a second linear diffusion unit configured to perform a linear diffusion process over data output

from the second nonlinear transformation units with respect to the range of the first subblock data, and

wherein at least one bit of data input to one of the second nonlinear transformation units in each of the encrypting sections is transmitted to at least one bit of data input to one of the second nonlinear transformation units in the succeeding encrypting section via at least two routes.

5. The apparatus according to claim 4, wherein the second nonlinear transformation unit in the first nonlinear transformation unit comprises a first-half second nonlinear transformation units preceding the second linear diffusion unit and second-half second nonlinear transformation units succeeding the second linear diffusion unit, and

the first linear diffusion unit in each of the encrypting sections supplies an exclusive OR value of at least two outputs from the second-half second nonlinear transformation units to at least one input to the first-half second nonlinear transformation units in the succeeding encrypting section.

6. The apparatus according to claim 4, wherein the second nonlinear transformation unit in the first nonlinear transformation unit comprises a first-half second nonlinear transformation units preceding the second linear diffusion unit and second-half second nonlinear transformation units succeeding the second

linear diffusion unit, and

the first linear diffusion unit in each of the encrypting sections supplies each exclusive OR value of at least two outputs from the second-half second nonlinear transformation units to each input to the first-half second nonlinear transformation units in the succeeding encrypting section.

7. The apparatus according to claim 4, wherein each of the first subblock data has equal bit length and each of the second subblock data has equal bit length, and

the first linear diffusion unit performs a linear diffusion process on a bit group formed of corresponding bits each extracted from a respective one of the second subblock data while changing a bit extracted position.

8. The apparatus according to claim 7, wherein the block data is 128 bits in length, each of the first subblock data is 32 bits in length, and each of the second subblock data is 8 bits in length,

the first linear diffusion unit performs a linear diffusion process on eight 16-bit data formed of corresponding bits each extracted from a respective one of sixteen second subblock data while changing a bit extracted position.

9. The apparatus according to claim 4, wherein the first linear diffusion unit is implemented by

hardware.

10. The apparatus according to claim 9, wherein an input-output characteristic of the first linear diffusion unit is based on multiplication over the
5 Galois field.

11. The apparatus according to claim 5, wherein the first linear diffusion unit is implemented by software.

12. An encryption apparatus based on a block
10 encryption scheme comprising:

encrypting sections connected in series in which the first section receives 128-bit plaintext and each of the second section and later sections receives 128-bit block data processed by the preceding section,
15 each of the encrypting sections comprising four first nonlinear transformation units each of which performs a local linear diffusion process and a nonlinear transformation process a corresponding one of four sets of 32-bit data into which 128-bit block data is
20 divided; and a first diffusion unit for performing a linear diffusion process using a maximum distance separable matrix on 128-bit block data in which four sets of 32-bit data output from the four first nonlinear transformation units are concatenated and
25 outputting the processed 128-bit block data to the next stage;

four first nonlinear transformation units which

are connected to first diffusion unit in the last encryption unit and receive 128-bit block data output from the first diffusion unit; and

5 a first key addition unit configured to receive four sets of 32-bit data output from the four first nonlinear transformation units and output 128-bit encrypted block data by adding 128-bit extended key data to 128-bit block data which is obtained by concatenating the four sets of 32-bit data output from
10 those four first nonlinear transformation units,

wherein each of the first nonlinear transformation units comprises four second key addition units each of which adds 8-bit key data to a corresponding one of four sets of 8-bit data into which the 32-bit data is
15 divided, four second nonlinear transformation units each of which performs nonlinear transformation on a corresponding one of the outputs of the second key addition units, a second diffusion unit for performing a linear diffusion process using a maximum distance
20 separable table on 32-bit data obtained by concatenating the four sets of 8-bit data output from the four second nonlinear transformation units, and four sets of third key addition units and a third nonlinear transformation units connected to follow the
25 second diffusion unit,

each of the first diffusion unit comprises a 16-bit diffusion unit for each of 8 bits for the second

nonlinear transformation units in preceding and succeeding stages, the 16-bit diffusion unit performing a linear diffusion process through a 4×4 matrix operation based on multiplication over the Galois field $GF(2^4)$ or its equivalent circuit, the matrix operation being such that four bits at corresponding bits positions in four sets of 8-bit data from the four second nonlinear transformation units in one first nonlinear transformation section in the preceding stage are taken as one element on the input side of the matrix operation and four bits at corresponding bit positions in four sets of 8-bit data input to the four second nonlinear transformation section in one first nonlinear transformation processing section in the succeeding stage are taken as one element on the output side of the matrix operation, and

in the 4×4 matrix operation based on multiplication over the Galois field $GF(2^4)$ in the 16-bit diffusion unit or its equivalent circuit transmitting, in any combination of one bit in the outputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the preceding stage and one bit in the inputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the succeeding stage, the state of that one bit in the

preceding stage to that one bit in the succeeding stage is transmitted over a plurality of operations paths.

13. An encryption apparatus based on common-key block encryption scheme comprising:

5 encrypting sections connected in series in which the first section receives 64-bit plaintext and each of the second section and later sections receives 64-bit block data processed by the preceding section, each of the encrypting sections comprising two first nonlinear
10 transformation units each of which performs a local linear diffusion process and a nonlinear transformation process a corresponding one of two sets of 32-bit data into which 64-bit block data is divided; and a first
15 diffusion unit for performing a linear diffusion process using a maximum distance separable matrix on 64-bit block data in which two sets of 32-bit data output from the two first nonlinear transformation units are concatenated and outputting the processed 64-bit block data to the next stage;

20 four first nonlinear transformation units which are connected to first diffusion unit in the last encryption unit and receive 64-bit block data output from the first diffusion unit; and

25 a first key addition unit configured to receive two sets of 32-bit data output from the two first nonlinear transformation units and output 64-bit encrypted block data by adding 64-bit common key data

to 64-bit block data which is obtained by concatenating the two sets of 32-bit data output from those two first nonlinear transformation units,

wherein each of the first nonlinear transformation
5 units comprises four second key addition units each of which adds 8-bit key data to a corresponding one of four sets of 8-bit data into which the 32-bit data is divided, four second nonlinear transformation units
10 each of which performs nonlinear transformation on a corresponding one of the outputs of the second key addition units, a second diffusion unit for performing a linear diffusion process using a maximum distance separable table on 32-bit data obtained by
15 concatenating the four sets of 8-bit data output from the four second nonlinear transformation units, and four sets of third key addition units and a third nonlinear transformation units connected to follow the second diffusion unit,

each of the first diffusion unit comprises a
20 16-bit diffusion unit for each of 8 bits for the second nonlinear transformation units in preceding and succeeding stages, the 16-bit diffusion unit performing a linear diffusion process through a 2×2 matrix operation based on multiplication over the Galois field
25 $GF(2^4)$ or its equivalent circuit, the matrix operation being such that four bits at corresponding bits positions in four sets of 8-bit data from the four

second nonlinear transformation units in one first nonlinear transformation section in the preceding stage are taken as one element on the input side of the matrix operation and four bits at corresponding bit positions in four sets of 8-bit data input to the four second nonlinear transformation section in one first nonlinear transformation processing section in the succeeding stage are taken as one element on the output side of the matrix operation, and

in the 2×2 matrix operation based on multiplication over the Galois field $GF(2^4)$ in the 16-bit diffusion unit or its equivalent circuit transmitting, in any combination of one bit in the outputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the preceding stage and one bit in the inputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the succeeding stage, the state of that one bit in the preceding stage to that one bit in the succeeding stage is transmitted over a plurality of operations paths.

14. A method for encrypting block data comprising:

randomizing first subblock data which are obtained by dividing the block data;

diffusing the randomized data with respect to a range which is wider than a range of the first subblock

data;

repeating the randomizing and the diffusing,
wherein at least two bits of the randomized data is
reflected on one bit of data to be randomized next.

5 15. An article of manufacture comprising a
computer readable medium having a computer program
embodied therein, the computer program comprising:

computer readable program code means for causing a
computer to randomize first subblock data which are
10 obtained by dividing plaintext block data;

computer readable program code means for causing a
computer to diffuse the randomized data with respect to
a range which is wider than a range of the first
subblock data; and

15 computer readable program code means for causing a
computer to repeat the randomizing and the diffusing,
wherein at least two bits of the randomized data is
reflected on one bit of data to be randomized next.

20 16. An apparatus for decrypting encrypted block
data comprising:

decrypting sections connected in series, each of
the decrypting sections comprising:

a first unit configured to randomize first
subblock data which are obtained by dividing encrypted
25 block data; and

a second unit configured to diffuse data output
from the first unit with respect to a range which is

wider than a range of the first subblock data and supply a result of diffusion to a first unit in a succeeding encrypting section, at least one bit of data input to the first unit in own encrypting section being
5 transmitted to at least one bit of data input to the first unit in the succeeding encrypting section via at least two routes.

17. A method for decrypting encrypted block data comprising:

10 randomizing first subblock data which are obtained by dividing encrypted block data;

diffusing the randomized data with respect to a range which is wider than a range of the first subblock data;

15 repeating the randomizing and the diffusing, wherein at least two bits of the randomized data is reflected on one bit of data to be randomized next.

18. An article of manufacture comprising a computer readable medium having a computer program
20 embodied therein, the computer program comprising:

computer readable program code means for causing a computer to randomize first subblock data which are obtained by dividing encrypted block data;

25 computer readable program code means for causing a computer to diffuse the randomized data with respect to a range which is wider than a range of the first subblock data; and

computer readable program code means for causing a computer to repeat the randomizing and the diffusing, wherein at least two bits of the randomized data is reflected on one bit of data to be randomized next.

104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000